International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Comparative Study of Image Steganography and Text Cryptography

Shabina N. Ahmed[1], Vinod Todwal[2]
[1]*M. Tech. Scholar, Dept. of Computer Science, Rajasthan College of Engineering for Women, Jaipur, India*
[2]*Asst. Professor, Dept. of Information Technology, Rajasthan College of Engineering for Women, Jaipur, India*

***Abstract*: Image steganography and text cryptography are two major techniques or methods for data security. Image steganography is bit more complex as it requires to deal with the frequency domain of the pixel values which forms the images, also it requires the special arrangements for the preservation of the RGB plane of the color images. Text cryptography on the other hand is a simpler in comparison to the image steganography as it does not require any special series or any complex equations to get processed for the inclusion of the secrete message, though the complex the mathematical model is, safer and effective will be the cryptographic data.**

***Keywords*: DWT, DCT, Reverse Mathematics, ASCII Codes.**

1. Introduction

THE basic structure of Steganography is made up of three components: the "carrier", the message, and the key1. The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will 'carry' the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light, or even lemon juice.

Image Steganography has many applications, especially in today's modern, hightech world. Privacy and anonymity is a concern for most people on the internet. Image Steganography allows for two parties to communicate secretly and covertly. It allows for some morally-conscious people to safely whistle blow on internal actions; it allows for copyright protection on digital files using the message as a digital watermark. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international governments. While Image Steganography has many legitimate uses, it can also be quite nefarious. It can be used by hackers to send viruses and trojans to compromise machines, and also by terrorists and other organizations that rely on covert operations to communicate secretly and safely.

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

2. Literature review

In the literature, many authors have tried to exploit the features of EC field to deploy for security applications. We have outlined some of the highlights of the relevant work in this section. M. Aydos et.al. [1] has presented an implementation of ECC over the field GF(p) on an 80 MHz, 32-bit RAM microprocessor along with the results. Kristin Lauter has provided an overview of ECC for wireless security [2]. It focuses on the performance advantages in the wireless environment by using ECC instead of the traditional RSA cryptosystem. Ray C., [3] in his work has explained the design of a generator, which automatically produces a customized ECC hardware that meets user-defined requirements. Alessandro Cilardo et al explains the engineering of ECC as a complex interdisciplinary research field encompassing such

fields as mathematics, computer science and electrical engineering [4]. C. J. McIvor et.al [5] introduces a novel hardware architecture for ECC over GF(p). The work presented by Gang Chen presents a high performance EC cryptographic process for general curves over GF(p) [6]. The standard standard specifications for public key cryptography is defined in [7].

A simple tutorial of ECC concept is very well documented and illustrated in the text authored by Williams Stallings et.al [8]. The paper presented by Kevin M. Finnigin et al outlines a brute-force attack on ECC implemented on UC Berkley's Tiny OS operating system for wireless sensor networks [9]. The attack exploits the short period of the pseudorandom number generators used by cryptosystem to generate private keys. An efficient and novel approach of a scalar point multiplication method than existing double and add by applying redundant recoding, which originates from radix-4 Booths algorithm was proposed by Sangook Moon [10]. In the paper as proposed by Jaewon Lee [11] presents 3 algorithms to perform scalar multiplication on EC defined over higher characteristic finite fields such as OEA (Optimal Extension Field). Liu Yongliang [12] showed that Aydos et al.' s protocol is vulnerable to man-in the-middle attack from any attacker but not restricted on the inside attacker. They proposed a novel ECC based wireless authentication protocol. A comprehensive coverage of EC field with the in-depth mathematical treatment is given in [13]. Owing to these existing works on ECC and its popularity, it is proposed to implement the crypto system based on ECC for text based application. The proposed work can be extended to XML based application since the future middleware technologies are in the control of XML based documents which is purely based on text.

Some of the popular approaches of text steganography:

A. *Line shift*

In this method, secret data is concealed by shifting the text lines vertically to some degree [14, 15]. A line noticeable has two unnoticeable control lines one on either sideways of it for spotting the direction of movement of the noticeable line [16]. To conceal a bit 0, upwards the line is shifted and to conceal bit 1, downwards the line is shifted [17]. Determination of where the line has been moved up or down is completed by determining the distance of the centroid of noticeable line and its control lines [16]. The hidden data would get damaged if the word is typed another time or if a (OCR) Character Recognition Program is used [14].

B. *Word shift*

In this method, secret text is secreted by horizontally shifting the words, i.e. right or left to symbolize bit 1 or 0 respectively [17]. Words shift are identified using correlation process that considers a profile as waveform and agrees whether it initiated from a waveform whose center slab has been moved left or right [16]. This technique can be recognized less, because variation of distance between words to fill a statement is very common [14], [15]. But if somebody identifies the procedure of distances, the person can compare or match the stego text with the algorithm and find the secreted content by the difference. Also, retyping or using OCR sequencers abolishes the concealed data [14], [15].

C. *Syntactic method*

This method uses marks of punctuation such as comma (,), full stop (.), etc. to hide bits 1 and 0. But problematic area with this technique is that it needs identification of right places to insert marks of punctuation [14], [15]. Hence, care must be done in applying this technique as person who reads can notify incorrect placement of punctuations [24].

D. *White steg*

This method uses white spaces for concealing a secret data. There are three means of hiding information by using white spaces. In Inter Sentence Spacing, insertion a single space to cover bit 0 and two spaces to conceal bit 1 at the end of individually terminating character [24]. In End of Line (EOL) at the last of every line spaces, insertion of fixed number of spaces is done. Just like, two spaces to convert one bit per line, four spaces to convert two bits and go on. In Inter Word Spacing method, one space afterward a word denotes bit 0 and two spaces afterward a word denotes bit 1. But, uneven use of white space is not transparent [24].

E. *Spam text*

To cover bits HTML and XML files can be used also. If there are several opening and closing tags, bit 0 is considered and if for starting and closing only tag is used, then bit 1 is considered [17]. In alternative method, bit 0 is denoted by a lack of space in a tag and bit 1 is denoted by placing a space inside a tag [17].

F. *SMS-texting*

SMS-Texting language is a grouping of shortened terms used in SMS [25]. Using full form of name or its abridged form binary data can be concealed. To store words and their respective shortened forms a Codebook is made. Full form of the word is used to hide bit 0, and abbreviated form of word is used to hide bit 1 [25].

G. *Feature coding*

In feature coding technique, the secret text is hidden by altering one or more characters of the text. All the features which can be used to conceal the information are surveyed and picked up by a parser in a text file [17]. Just like, points in letters ‘i’ and ‘j’ can be placed otherwise, length of strike can be altered in letters f and t, or by lengthening or shortening the height of letters ‘b’, ‘d’, ‘h’, etc. [26, 18]. There is an error in this process which is, if an OCR package is used or if re-writing has been done, the concealed message would get damaged.

H. *SSCE (Secret Steganographic Code for Embedding)*

This method first ciphers a data using Secret Steganographic Code for Embedding table and then encapsulates the encrypted

text in a face file by putting articles a or an with the non-precise nouns in English language using a definite mapping system [19]. The embedding positions are ciphered using the similar SSCE table and set aside in other file which is transmitted to the recipient with the stego file surely.

I. Word mapping

In this method a secret message is ciphered using inherited operative crossover and then inserts the resultant cipher text, using two bits at a time, in a mask file by putting blank spaces in between words of even or odd length by means of some mapping method [20]. The embedding positions are stored in some another file and sent to the recipient along with the stego entity.

J. MS Word document

In this method, text sections in an article are deteriorated, imitating to be the work of a writer with substandard writing skills, with confidential text being concealed in the choice of deteriorations which are then reviewed with modifications being traced [21]. Data inserting is concealed such that the stego article seems to be the product of combined writing [21].

K. Cricket match scorecard

In this technique, data is concealed in a cricket match record by earlier appending a useless zero previous to a number to symbolize bit 1 and parting the number as it is to signify bit 0 [22].

L. CSS (Cascading Style Sheet)

This method scrambles a data using RSA public key cryptosystem and secret message text is then fixed in a Cascading Style Sheet (CSS) by using End of Line on each CSS style properties, closely after a (;) semicolon. A space afterward a semicolon inserts bit 0 and a double space afterward a semicolon inserts bit 1 [23].

3. Conclusion

After studying out the various papers about the steganography and cryptography for images and for text it can be deduced that still a lot of work and techniques are yet to be explored and flourished in this field of data security, however eliminating the use of public key for encryption and encapsulating the secrete data of any length are the biggest challenge as per the current scenarios and requirements.

References

[1] M.Aydos, T.Yanik and C.K.Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor," IEE Proc Commun.,Vol. 148, No.5, pp. 273-279, October 2001.
[2] Kristin Lauter, "The Advantages of Elliptic Cryptography for Wireless Security", IEEE Wireless Communications, pp. 62- 67, Feb. 2006.
[3] Ray C. C. Cheng, Nicolas Jean-baptiste, Wayne Luk, and Peter Y. K Cheung,"Customizable Elliptic Curve Cryptosystems", IEEE Trans. On VLSI Systems, vol. 13, no. 9, pp. 1048-1059, Sep. 2005.
[4] Alessandro Cilardo, Luigi Coppolino, Nicola Mazzocca, and Luigi Romano,"Elliptic Curve Cryptography Engineering", Proceedings of the IEEE, Vol. 94, no. 2, pp. 395 - 406, Feb. 2006.
[5] C. 1. McIvor, M. McLoone, and 1. V. McCanny, "Hardware elliptic curve cryptographic processor over GF(p)," IEEE Trans. Circuits Syst.l Reg. Papers, vol. 53, no. 9, pp. 1946-1957, Sep. 2006.
[6] Gang Chen, Guoqiang Bai, and Hongyi Chen, " A High-Performance Elliptic Curve Cryptographic Processor for General Curves Over GF(p) Based on a Systolic Arithmetic Unit", IEEE Trans. Circuits Syst. - 11: Express Briefs, vol. 54, no. 5, pp. 412- 416, May. 2007.
[7] Standard specifications for public key cryptography, IEEE standard, pI363,2000.
[8] Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.
[9] Kevin M. Finnigin, Barry E. Mullins, Richard A. Raines, Henry B.Potoczny, "Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks," Internationaljournal ofsecurity and networks, Vol. 2, No. 3/4, pp. 260- 271,2006.
[10] Sangook Moon, "A Binary Redundant Scalar Point Multiplication in Secure Elliptic Curve Cryptosystems," International journal of network security, Vol.3, No.2, PP.132-137, Sept. 2006.
[11] Jaewon Lee, Heeyoul Kim, Younho Lee, Seong-Min Hong, and Hyunsoo Yoon, "Parallelized Scalar Multiplication on Elliptic Curves Defined over Optimal Extension Field," International journal of network security, VolA, No.1, PP.99-106, Jan. 2007.
[12] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu, "Elliptic Curve Cryptography Based Wireless Authentication Protocol," International journal ofnetwork security, VolA, No.1, PP.99-106, Jan. 2007.
[13] R.V.Kurja, Kirti Joshi, N.Mohan Kumar, Kapil H Raranape, A.Ramanathan, T.N.Shorey, R.R.Simha, and V.Srinivas, Elliptic Curves, International Distribution by American Mathematical Society, 2006. ICAC
[14] M. H. S. Shahreza, and M. S. Shahreza, "A new approach to Persian/Arabic text steganography", In Proceedings of 5th IEEE/ACIS Int. Conf. on Computer and Information Science and 1st IEEE/ACIS Int. Workshop on Component-Based Software Engineering, Software Architecture and Reuse, 2006, pp. 310-315.
[15] M. H. S. Shahreza, and M. S. Shahreza, "A new synonym text steganography," Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1524-1526, 2006.
[16] S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O. Gorman, "Document marking and identification using both line and word shifting," INFOCOM'95 Proceedings of the Fourteenth Annual Joint Conf. of the IEEE Computer and Communication Societies, pp. 853-860, 1995.
[17] J. Cummins, P. Diskin, S. Lau, and R. Parlett, "Steganography and digital watermarking," School of Computer Science, pp.1-24, 2004.
[18] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O. Gorman, "Electronic marking and identification techniques to discourage document copying," IEEE Journal on Selected Areas in Communication, vol.1, pp. 1495-1504, 1995.
[19] I. Banerjee, S. Bhattacharyya, and G. Sanyal, "Novel text steganography through special code generation," Int. Conf. on Systemics, Cybernetics and Informatics, pp. 298-303, 2011.
[20] S. Bhattacharyya, I. Banerjee, and G. Sanyal, "A novel approach of secure text based steganography model using word mapping method," Int. Journal of Computer and Information Engineering, vol.4, pp. 96-103, 2010.
[21] T. Y. Liu, and W. H. Tsai, "A new steganographic method for data hiding in Microsoft word documents by a change tracking technique," IEEE Transactions on Information Forensics and Security, vol.2, no.1, pp. 24-30, 2007.
[22] M. Khairullah, "A novel text steganography system in cricket match scorecard", Int. Journal of Computer Applications, vol.21, pp. 43-47, 2011.
[23] H. Kabetta, B. Y. Dwiandiyanta, and Suyoto, "Information hiding in CSS: a secure scheme text steganography using public key cryptosystem," Int. Journal on Cryptography and Information Security, vol.1, pp. 13-22, 2011.
[24] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol.35, pp. 313- 336, 1996.
[25] M. S. Shahreza, and M. H. S. Shahreza, "Text steganography in SMS", 2007 Int. Conf. on Convergence Information Technology, 2007, pp. 2260-2265.

[26] K. Rabah, "Steganography-the art of hiding data", Information Technology Journal, vol.3, pp. 245-269, 2004.